Ontario

Ministry of Agriculture, Food and Rural Affairs

central site | feedback | search | site map | français

HOME | WHAT'S NEW | CALENDAR | PRODUCTS | NEWS RELEASES

FACTSHEET

ISSN 1198-712X ©Queen's Printer for Ontario

Agdex#: 057 Publication Date: August 2005

Order#: 05-049 Last Reviewed: August 2005

# Title: Personal Information Protection and Electronic Documents Act

**Division:** Innovation and Competitiveness

**History:**

**Written by:** Denise Edwards - Agriculture Organization Specialist/OMAFRA

## Table of Contents

1. Introduction
2. What is Personal Information?
3. Does PIPEDA Apply to Your Organization?
4. Principles of PIPEDA
5. How to Comply with PIPEDA
6. Role of Board of Directors
7. Acknowledgements
8. Related Links

## Introduction

The Personal Information Protection and Electronic Documents Act (PIPEDA) is federal legislation passed in 2001 and fully implemented on January 1, 2004. While some provinces have passed their own privacy legislation, Ontario has not, so the federal legislation applies here. Increasingly, organizations and businesses rely on personal information to connect with their customers and members. Respecting and protecting customers' and members' privacy is part of good customer and member relations.

The purpose of the Act is "to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

PIPEDA requires that you:

- obtain the clear consent of an individual before you collect, use or disclose personal information about that individual
- use the information only for the purposes for which you have consent
- protect the information from unauthorized access and use
- keep the information up to date and correctly filed so that decisions are based on correct information
- destroy information when you no longer need it for the original purpose and
- implement accountability mechanisms in your organizations to ensure compliance with the above.

Note: The legislation is intricate, so be sure to obtain legal advice to fully understand the requirements. As legislation is reviewed and amended periodically, ensure you are referring to the most current version.

## What Is Personal Information?

The Act aims to protect information about an individual, including information such as:

- age, name, income, ethnic origin, religion or blood type
- opinions, evaluation, comments, social status or disciplinary actions
- credit records, employment history and medical records.

Personal information does not include the name, title, business address or telephone number of an employee of an organization.

For many organizations, this means that the information collected to establish eligibility for membership, programs, donor histories, personnel files of staff and volunteers may be considered personal information.

## Does PIPEDA Apply To Your Organization?

PIPEDA applies to most organizations and businesses in Ontario that are conducting "commercial activity," with commercial activity being defined very broadly. The law affects the way organizations collect, use and disclose personal information about individuals. You will have to comply with PIPEDA if your organization engages in "commercial activity," which is defined in Section 2 as:

" . . . any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

According to the Office of the Privacy Commissioner of Canada in the Factsheet "The Application of the PIPEDA to Charitable and Non-Profit Organizations," a non-profit organization is not automatically exempt. Most non-profits such as charities, minor hockey associations, clubs, community groups and advocacy organizations are not subject to the *Act* because they do not engage in commercial activities. Collecting membership fees, organizing club activities, compiling a list of members' names and addresses, and mailing out newsletters are not considered commercial activities. Fundraising is not considered a commercial activity unless lists are exchanged.

Some clubs may be engaged in commercial activities by selling, bartering or leasing a membership list or a list of donors. In these situations, consent is required for the disclosure of the information. Assuming the information is not considered sensitive, an organization can use a clear, simple and easy-to-execute opt-out process as a means of obtaining consent.

Although the *Act* may not apply to charities, associations and other similar organizations, it is recommended that such organizations provide their members, donors or supporters with an opportunity to decline to receive further communications. If you have paper or computer files that contain information about your employees, clients, donors, volunteers, exhibitors or others, your method of collecting, protecting and using that information must comply with the Act.

## Principles Of PIPEDA

The Act is based on 10 principles that are applied to an organization's activities.

1. **Accountability:** An organization is responsible for the personal information under its control and shall designate an individual who is responsible for the organization's compliance. This Chief Privacy Officer will understand the policies and procedures and deal with complaints.
2. **Identify Purposes:** The purposes for which the information is collected should be identified on or at the time of collection. Organizations should develop "purpose statements."
3. **Consent:** The knowledge and consent of the individual are required for collection, use or disclosure of personal information in a commercial activity. Consent can be expressed or implied. The Privacy Commissioner recommends expressed consent in most instances. Some examples of expressed consent are:

- An individual completes and signs a form giving consent to the collection of information for

specified purposes, its use and if it is to be disclosed.
- A check-off box allows individuals to request their personal information not be given.
  Note: Although entering into competitions may be classified as implying consent, this is not clear enough, and organizations are advised to include consent in their rules and on their exhibitor registration forms.

4. **Limiting Collection:** Information is to be collected for specific purposes and can only be used for those purposes. Information cannot be collected by misleading or deceiving the individuals about the purpose for which it is intended.
5. **Limiting Use, Disclosure and Retention of Personal Information:** Organizations can only use, disclose and retain personal information for the specific purposes it was collected for and must not retain it longer than needed for those specific purposes.
6. **Accuracy**: Personal information shall be accurate, complete and up to date.
7. **Safeguards:** The organization must protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification. The level of security should be appropriate to the sensitivity of the information. People with access should sign confidentiality agreements.
   Note: The organization should ensure the security of its computers and paper files.
8. **Openness:** The organization's privacy policies must be readily available to anyone.
9. **Individual Access:** Individuals have the right to know what personal information about them has been collected, how it is being used, to whom it has been disclosed, and to challenge the accuracy and completeness and to have errors corrected.
10. **Challenging Compliance**: Individuals should be able to address any challenges concerning compliance to the organization's Chief Privacy Officer.

## How To Comply With PIPEDA

The principles of PIPEDA make good sense for any organization that relies upon the trust of donors, clients and the community. If you're starting from scratch, following the steps listed below should help your organization comply with the spirit and intent of the Act.

1. Ensure you understand the Act and the principles set out in it. The web sites listed at the end of this Factsheet contain links to the official version, commentary and legal interpretations of the principles. Seek legal advice to determine how specific points may affect your organization
2. Appoint a compliance officer. This should be someone who has authority in the organization and can deal with the public.
3. Conduct a review of your organization's current practices concerning the personal information it collects and maintains. Some of the questions you should be asking include:

- What personal information is collected and why?
- How is it collected?
- What is it used for?
- How do we ensure that it can only be used for the intended purposes?
- How do we ensure that we have the consent of the individual to collect and use the information?
- Where is this information kept now?
- Who has access?
- What security measures are in place?
- With whom do we share the information?
- What do we do with the information when it is no longer needed?

1. Based upon the review, develop a privacy policy, consent mechanism and complaints process.
2. Update any forms (paper and electronic) that you use to collect personal information, i.e., exhibitor's registration cards and contracts you have with employees, suppliers, marketing firms, fundraising companies and other organizations that involve the collection or transfer of personal information.
3. Ensure you have a way to deal with opt-outs. You don't want to be sending appeal letters to people who have said they don't want to receive them.
4. Update your data security systems and file management procedures to ensure that personal information is protected from unauthorized access.
5. 
6. Train your employees and volunteers. If they have access to personal information, they should

sign a confidentiality agreement statement and have a good understanding of your policies and practices. They should know who is responsible for dealing with inquiries and complaints.

7. Make your policy available. It should be easily accessible to anyone who wants to see it.

## Role Of Board Of Directors

- Ensure that directors receive appropriate training in privacy concepts and that there is some privacy expertise on their board.
- Ensure that at least one person has been designated to be acccountable for the organization's privacy compliance.
- If it is a staff person who is assigned the responsibility, ensure that privacy compliance is a part of their performance evaluation and compensation.
- Undertake periodic privacy self-assessments and audits of directors and report to the board on a regular basis.

Some examples of privacy policies for organizations can be found on the following web sites:
(all links are found in related links section)

ARMA International

4-H Ontario

World Wildlife Fund

Compasstax Chartered Accountants

An article on data security entitled "Basic Information Security" is available at http://www.peaceworks.ca/ under "articles."

## Acknowledgements

The author would like to acknowledge the following resources that were used in the development of this Factsheet and encourage people to refer to the web sites for more information.

### The Act

"Personal Information Protection and Electronic Documents Act." Government of Canada. 2000. http://www.parlc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html

Easier-to-read-online version is on the web site of the Office of the Privacy Commissioner of Canada: http://ww.pivcom.gc.ca/legislation/02_06_01_01_e.asp

### Other Resources

"Application of the Personal Information Protection and Electronic Documents Act to Charitable and Non-Profit Organizations." Factsheet. Office of the Privacy Commissioner of Canada. May 2004. http://www.privcom.gc.ca/fs-fi/02_05_d_19_e.asp

"Court Considers Application of PIPEDA to Non-Profit Club." The Canadian Association. January 2005. Rachel Bumenfeld.
http://www.axi.ca/tca/Jan2005/guestarticle_6.shtml

Focus on Privacy — Does PIPEDA Apply to My Company? McInnes Cooper. September 2003. David T.S. Fraser.
http://www.mcinnescooper.com/publications2.asp?id=56

"Donor Lists Protected as Charitable Property Under Canadian Law." Charity Law Bulletin. No. 15, July 25, 2002. Jacqueline M. Connor, Mervyn F. White, and Terrance S. Carter.
http://ww.caters.ca/pub/bulletin/charity/2002/chylb15.htm

"Impact of the Personal Information Protection and Electronic Documents Act (PIPEDA) on Charitable and Non-Profit Organizations." The Canadian Association. 2003. Mark Wong and others.
http://www.axi.ca/TCA/Jan2004/guestarticle_5.shtml

The PIPEDA Privacy Principles: A Guide for Associations and Nonprofit Organizations. Association Xpertise Inc. 2001.
http://www.axi.ca/esDocs/Privacy_Guide.pdf

"Privacy 101: A Guide to Privacy Legislation for Fundraising Professionals and Not-For-Profit Organizations in Canada." Version I. Prepared by a cross-sector working group representing: Association of Fundraising Professionals (AFP), Association for Healthcare Philanthropy (AHP), Association of Professional Researchers for Advancement (APRA), and Canadian Centre for Philanthropy (CCP).
http://www.aforonto.org/new_on_site/Privacy101.pdf

"Privacy and Boards of Directors: What You Don't Know CAN Hurt You." Information and Privacy Commissioner/Ontario. November 2003. Ann Cavoukian.
http://www.ipc.on.ca/docs/director.pdf

"Privacy Compliance: What Churches and Charities Need to Do by January 1, 2004." The 2003 Annual Church and the Law Seminar. Power Point Presentation. November 2003. Mark J. Wong.
http://www.caters.ca/pub/seminar/chrchlaw/2003/mjw_priv.pdf

"Privacy Law and Governance in the Non-Profit Sector." Charity Village News Week. October 20, 2003. Jeffrey H. McCully.
http://www.hrityvillage.com/cv/archive/acov/acov03/acov0334.html
http://ww.carityvillage.com/cv/archive/acov/acov03/acov0336.html

"Special Issue on Complying With the Personal Information Protection and Electronic Documents Act." Nonprofit News from Nathan: December 2003. Nathan Garber & Associates. Nathan Garber.
http://garbercsulting.com/nonprofit_news_03_12.htm

Disclaimer: The purpose of this Factsheet is to inform organizations about this important federal legislation. This document is for general information and should not be relied upon as legal advice. The legislation is intricate; consult with your lawyer as to how it may affect your organization.

## Related Links

- ARMA International
- 4-H Ontario
- World Wildlife Fund
- Compasstax Charterd Accountants
- Basic Information Security

| Top of Page |

For more information:
Toll Free: 1-877-424-1300
Local: (519) 826-4047
Email: ag.info@omaf.gov.on.ca

Ontario
This site is maintained by the Government of Ontario, Canada.

This information is provided as a public service, but we cannot guarantee that the information is current or accurate.
Readers should verify the information before acting on it.

Feedback and technical inquiries to: rural@omaf.gov.on.ca
© Copyright 2005 Queen's Printer for Ontario
Last Updated: October 14, 2005

FICHE TECHNIQUE

COMMANDE N° 05-050

AOÛT 2005

AGDEX 057

Ontario

Ministère de l'Agriculture, de l'Alimentation et des Affaires rurales

# LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES

**D. Edwards**

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) est une loi fédérale qui a été adoptée en janvier 2001 et qui est entrée en vigueur dans son intégralité le 1er janvier 2004. Comme l'Ontario n'a pas adopté de loi provinciale sur la protection des renseignements personnels, la LPRPDÉ s'applique dans notre province. Il devient sans cesse plus indispensable aux organisations et aux entreprises d'avoir des données personnelles sur leurs clients et leurs membres pour rester en communication avec eux. Or, le respect et la protection des renseignements personnels est une composante à part entière des bonnes relations avec les clients et les membres.

L'objet de la LPRPDÉ est « de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ».

La LPRPDÉ vous impose :

- d'obtenir le consentement clair de toute personne avant de recueillir, d'utiliser ou de divulguer des renseignements la concernant;
- de ne les utiliser qu'aux fins mises en avant quand la personne vous a donné son consentement;
- de les protéger contre tout accès ou utilisation non autorisée;
- de les tenir à jour et d'en assurer l'exactitude afin que des décisions ne soient pas prises à partir de renseignements erronés;
- de les détruire dès que vous n'en avez plus besoin pour atteindre les fins mises en avant;
- de mettre en œuvre, dans votre organisation, des mécanismes de responsabilisation pour assurer le respect des exigences énoncées ci-dessus.

**Remarque :** La LPRPDÉ est complexe, aussi devriez-vous demander l'aide d'un conseiller juridique pour en saisir toutes les exigences. En outre, comme elle est périodiquement réexaminée et modifiée, assurez-vous d'avoir en main la dernière version en date.

## QU'EST-CE QU'UN RENSEIGNEMENT PERSONNEL?

La Loi a pour objet la protection des renseignements propres à l'individu, notamment :

- âge, nom, revenu, origine ethnique, religion ou type sanguin
- opinions, évaluation, commentaires, statut social ou mesures disciplinaires
- antécédents de crédit, antécédents d'emploi et dossier médical.

Le nom, le titre, l'adresse ou le numéro de téléphone au travail des employés d'une organisation ou d'une entreprise ne sont pas des renseignements personnels.

Pour beaucoup d'organisations, cela signifie que les renseignements qu'elles ont recueillis pour établir l'admissibilité au statut de membre ou à des programmes, les historiques des donateurs et les dossiers des membres du personnel et des bénévoles pourraient être tenus pour des renseignements personnels.

## LA LOI S'APPLIQUE-T-ELLE À VOTRE ORGANISATION?

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) s'applique à la plupart des organisations et des entreprises de l'Ontario qui

exercent une « activité commerciale », notion à laquelle la Loi donne un sens très large. Elle dicte les conditions dans lesquelles les organisations doivent recueillir, utiliser et divulguer les renseignements concernant les personnes. Est tenue de se conformer à la LPRPDÉ toute organisation qui exerce une « activité commerciale » au sens de l'article 2 de la Loi :

> « activité commerciale : Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de liste de donneurs, d'adhésion ou de collecte de fonds. »

Selon la fiche d'information « Application de la *Loi sur la protection des renseignements personnels et les documents électroniques* aux œuvres de charité et aux organisations sans but lucratif », publiée par le Commissariat à la protection de la vie privée du Canada, une organisation sans but lucratif n'est pas automatiquement dispensée des obligations découlant de la Loi. La plupart des organisations sans but lucratif ne sont pas assujetties à la Loi parce qu'elles n'exercent pas d'activités commerciales. C'est généralement le cas de la majorité des œuvres de charité, des associations de hockey mineur, des clubs, des groupes communautaires et des organisations de défense des droits. La perception de droits d'adhésion, l'organisation d'activités de club, l'établissement d'une liste de noms et d'adresses de membres et l'envoi de bulletins de nouvelles n'entrent pas dans la définition de l'activité commerciale. La collecte de fonds n'est pas non plus considérée comme une activité commerciale, à moins qu'il n'y ait échange de listes.

Certains clubs peuvent exercer des activités commerciales s'ils vendent, troquent ou prêtent des listes de membres ou de donateurs. Avant de se livrer à ce type d'activités, il faut que le club ait obtenu le consentement de ses membres ou de ses donateurs. Sauf si les renseignements sont considérés « sensibles », une organisation peut demander à ses membres ou donateurs de signifier leur consentement (ou leur refus) par un moyen clair, simple et facile à exécuter.

Bien que la Loi puisse ne pas s'appliquer à elles, les œuvres de charité, les associations et autres organisations similaires ont intérêt à permettre à leurs membres, donateurs et sympathisants de faire savoir s'ils refusent d'être sollicités à nouveau. Si vous conservez en dossiers électroniques ou sur papier des renseignements sur vos employés, clients, donateurs, bénévoles, exposants ou autres, vous devez veiller à ce que votre méthode de collecte, de protection et d'utilisation de ces renseignements soit conforme à la Loi.

## PRINCIPES DE LA LPRPDÉ

La Loi repose sur dix principes qui s'appliquent aux activités des organisations.

1. **Responsabilisation** Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner la personne qui devra s'assurer du respect des principes de la Loi. La personne chargée au premier chef de la protection des renseignements personnels dans une organisation doit maîtriser les politiques et les méthodes en la matière et répondre aux plaintes.

2. **Détermination des fins de la collecte des renseignements** Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci. Les organisations sont tenues d'énoncer ces fins par écrit.

3. **Consentement** Toute personne doit être informée de toute collecte, utilisation ou communication à des fins commerciales de renseignements personnels qui la concernent et y consentir. Le consentement peut être explicite ou implicite. Cependant, le commissaire à la protection de la vie privée recommande que le consentement soit obtenu de façon explicite dans la majorité des cas. Voici des exemples de la forme que peut revêtir le consentement explicite :

   - La personne remplit et signe un formulaire signifiant qu'elle consent à la collecte et à l'utilisation des renseignements à des fins précises et, le cas échéant, à leur communication à des tiers.
   - La personne peut cocher une case pour exiger que les renseignements la concernant ne soient pas communiqués à des tiers.

   **Remarque** : Le fait de remplir un formulaire de participation à un concours peut être interprété comme un consentement implicite, mais, cela n'étant pas clair, on conseille aux organisations d'inclure une clause sur le consentement dans les règles de concours et les formulaires d'inscription.

4. **Limitation de la collecte des renseignements** Une organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et elle ne peut les utiliser qu'à ces fins. Il est interdit de recueillir des renseignements en trompant les personnes sur le but de cette collecte.

5. **Limitation de l'utilisation, de la communication et de la conservation des renseignements** Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles qui ont été déterminées. On ne doit conserver les renseignements

personnels que pendant la période nécessaire pour atteindre les fins déterminées.

6. **Exactitude** Les renseignements personnels doivent être exacts, complets et à jour.

7. **Mesures de sécurité** L'organisation doit protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis. Les personnes qui ont accès à ces renseignements doivent signer des ententes de confidentialité.

   **Remarque :** L'organisation doit empêcher l'accès à son matériel informatique et à ses dossiers sur papier.

8. **Transparence** L'organisation est tenue de mettre ses politiques sur la protection des renseignements personnels à la disposition de quiconque en fait la demande.

9. **Accès aux renseignements personnels** Toute personne a le droit de savoir quels renseignements ont été recueillis à son sujet, de quelle manière ils sont utilisés et à qui ils sont communiqués; elle doit aussi pouvoir contester l'exactitude et l'intégralité de ces renseignements et y faire apporter les corrections appropriées.

10. **Possibilité de porter plainte à l'égard du non-respect des principes** Toute personne doit pouvoir s'adresser à la personne qui, dans une organisation, est chargée au premier chef de la protection des renseignements personnels, afin de porter plainte pour non-respect de la LPRPDÉ.

## COMMENT SE CONFORMER À LA LPRPDÉ

Les principes de la LPRPDÉ tombent sous le sens pour toute organisation qui repose sur la confiance de ses donateurs, de ses clients et de la collectivité. Si votre organisme est novice en matière de protection des renseignements personnels, sa mise en conformité à l'esprit et à la lettre de la Loi sera simplifiée si vous suivez les étapes suivantes :

1. Assurez-vous de comprendre la Loi et les principes qu'elle énonce. Les sites Web indiqués à la fin de la présente fiche technique contiennent des liens menant à la version officielle de la Loi et à des commentaires et interprétations, formulées par des spécialistes, concernant les principes de la Loi. Demandez l'aide d'un conseiller juridique pour déterminer si votre organisation est visée par certains points précis de la Loi.

2. Désignez la personne qui, dans votre organisation, sera chargée de veiller au respect de la Loi. Ce doit être quelqu'un qui occupe un poste d'autorité et qui peut interagir avec le public.

3. Faites le point sur les pratiques suivies actuellement dans votre organisation relativement aux renseignements personnels qu'elle collecte et conserve. Réfléchissez aux questions suivantes :

   - Quels renseignements personnels recueillons-nous et à quelle fin?
   - Comment les recueillons-nous?
   - Quel usage en faisons-nous?
   - Que faisons-nous pour voir à ce qu'ils ne soient utilisés qu'à cette fin?
   - Comment vérifier que les intéressé(e)s ont consenti à la collecte et à l'utilisation des renseignements les concernant?
   - Où conservons-nous ces renseignements à l'heure actuelle?
   - Qui y a accès?
   - Quelles mesures de sécurité appliquons-nous?
   - Avec qui partageons-nous les renseignements?
   - Qu'en faisons-nous quand nous n'en avons plus besoin?

4. À partir de votre constat, mettez en place une politique de confidentialité et des mécanismes pour encadrer l'obtention du consentement et l'instruction des plaintes.

5. Mettez à jour tous les formulaires (sur papier et électroniques) que vous utilisez pour recueillir des renseignements personnels, par exemple, bulletins d'inscription des exposants à une foire) et tous les contrats que vous avez signés avec des employés, fournisseurs, agences de marketing, organisations de collecte de fonds et autres, et qui impliquent la collecte ou le transfert de renseignements personnels.

6. Créez un mécanisme pour éliminer de vos listes d'envoi les personnes ayant exigé d'en être rayées. Vous devez prendre garde de ne pas envoyer des demandes de dons à des personnes qui ont demandé à ne pas être sollicitées.

7. Mettez à jour vos systèmes de protection des données et vos méthodes de gestion des dossiers pour vous assurer que les renseignements personnels sont protégés contre tout accès non autorisé.

8. Donnez la formation nécessaire à vos employés et à vos bénévoles. Ceux et celles qui ont accès à des renseignements personnels devraient signer une entente de confidentialité et être au courant de vos politiques et de vos pratiques. Ils devraient savoir qui, dans votre organisation, est chargé de répondre aux demandes d'information et de traiter les plaintes.

9. Veillez à rédiger par écrit votre politique et à la rendre facilement accessible à quiconque en fait la demande.

## RÔLE DU CONSEIL D'ADMINISTRATION

- Veillez à ce que les membres du conseil d'administration reçoivent la formation nécessaire aux concepts de la confidentialité et à ce que certains soient compétents en la matière.
- Veillez à désigner au moins un responsable de la conformité de votre organisation à la LPRPDÉ.
- Si le responsable désigné est un membre du personnel, faites en sorte qu'il soit tenu compte de cette charge dans l'évaluation de son rendement et dans sa rémunération.
- Périodiquement, procédez à des auto-évaluations et à des vérifications auprès des membres du conseil d'administration sur la question du respect des renseignements personnels et présentez un rapport au conseil d'administration.

Les sites Web ci-après contiennent des exemples de politiques de confidentialité de certaines organisations :

- ARMA International
  http://www.arma.org/privacy/index.cfm
- 4-H Ontario
  http://www.4-hontario.ca/privacy.cfm
- Fonds mondial pour la nature Canada
  http://www.wwf.ca/AboutWWF/WhoWeAre/WhoWeAre.asp?page=security&lang=FR
- Compasstax Chartered Accountants
  http://www.compasstax.ca/priv_policy.php

Vous pouvez consulter l'article « Basic Information Security » contenant des renseignements de base sur la sécurité des données à http://www.peaceworks.ca/, sous la rubrique « articles ».

**REMERCIEMENTS**

L'auteure tient à remercier les organismes qui l'ont autorisée à se servir des ressources ci-dessous pour préparer la présente fiche technique et elle invite les personnes intéressées à consulter les sites Web suivants :

**La Loi**

*Loi sur la protection des renseignements personnels et les documents électroniques*. Gouvernement du Canada. 2000.
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-F.html

Une version de la Loi plus facile à consulter se trouve sur le site Web du Commissariat à la protection de la vie privée du Canada :
http://www.privcom.gc.ca/legislation/02_06_01_01_f.asp

**Autres ressources**

« Application de la *Loi sur la protection des renseignements personnels et les documents électroniques* aux œuvres de charité et aux organismes sans but lucratif ». Fiche d'information. Commissariat à la protection de la vie privée du Canada. Mai 2004.
http://www.privcom.gc.ca/fs-fi/02_05_d_19_f.asp

« Court Considers Application of PIPEDA ». *The Canadian Association*. Janvier 2005. Rachel Bumenfeld.
http://www.axi.ca/tca/Jan2005/guestarticle_6.shtml

« Focus on Privacy — Does PIPEDA Apply to My Company? » *McInnes Cooper*. Septembre 2003. David T.S. Fraser.
http://www.mcinnescooper.com/publications2.asp?id=56

« Donor Lists Protected as Charitable Property Under Canadian Law ». *Charity Law Bulletin*. N° 15, 25 juillet 2002. Jacqueline M. Connor, Mervyn F. White et Terrance S. Carter.
http://www.carters.ca/pub/bulletin/charity/2002/chylb15.htm

« Impact of the Personal Information Protection and Electronic Documents Act (PIPEDA) on Charitable and Non-Profit Organizations ». *The Canadian Association*. 2003. Mark Wong et coll.
http://www.axi.ca/TCA/Jan2004/guestarticle_5.shtml

« The PIPEDA Privacy Principles: A Guide for Associations and Non-profit Organizations ». *Association Xpertise Inc. 2001*.
http://www.axi.ca/ResDocs/Privacy_Guide.pdf

« Privacy 101: A Guide to Privacy Legislation for Fundraising Professionals and Not-For-Profit Organizations in Canada ». Version I. Rédigé par un groupe de travail intersectoriel représentant : *l'Association of Fundraising Professionals* (AFP), *l'Association for Healthcare Philanthropy* (AHP), *l'Association of Professional Researchers for Advancement* (APRA) et le *Centre canadien de philanthropie* (CCP).
http://www.afptoronto.org/new_on_site/Privacy101.pdf

« Privacy and Boards of Directors: What You Don't Know CAN Hurt You ». *Bureau du commissaire à l'information et à la protection de la vie privée/Ontario*. Novembre 2003. Ann Cavoukian.
http://www.ipc.on.ca/docs/director.pdf

« Privacy Compliance: What Churches and Charities Need to Do by January 1, 2004 ». *The 2003 Annual Church and the Law Seminar*. Présentation PowerPoint. Novembre 2003. Mark J. Wong.
http://www.carters.ca/pub/seminar/chrchlaw/2003/mjw_priv.pdf

« Privacy Law and Governance in the Non-Profit Sector ». *Charity Village News Week*. 20 octobre 2003. Jeffrey H. McCully.
http://www.charityvillage.com/cv/archive/acov/acov03/acov0334.html
http://www.charityvillage.com/cv/archive/acov/acov03/acov0336.html

« Special Issue on Complying With the Personal Information Protection and Electronic Documents Act. » *Nonprofit News from Nathan*: Décembre 2003. Nathan Garber & Associates. Nathan Garber.
http://garberconsulting.com/nonprofit_news_03_12.htm

Clause de non-responsabilité : La présente fiche technique entend fournir aux organisations une information de nature générale sur cette importante loi fédérale. Elle ne saurait se substituer à l'avis d'un spécialiste juridique. La Loi est complexe, aussi devriez-vous consulter votre conseiller juridique pour savoir en quoi elle s'applique à votre organisation.

Cette fiche technique a été rédigée par **Denise Edwards**, spécialiste du développement organisationnel en agriculture, Division de l'innovation et de la compétitivité, MAAARO, Guelph.

NOTES PERSONNELLES

Centre d'information agricole
1 877 424-1300
*ag.info@omafra.gov.on.ca*

**www.omafra.gov.on.ca**

POD
ISSN 1198-7138
Also Available in English
(Order No. 05-049)

Ontario

*01210100505050*